SPYWOLF

Security Audit Report

Completed on

July 24, 2023

OVERVIEW

This audit has been prepared for **KoKo** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

TABLE OF CONTENTS

KoKo

PROJECT DESCRIPTION

According to their website:

Everyone looks at cute dogs, hamsters, frogs and sadly regrets that they did not have time to “take” them for themselves.

More recently, they were the kings of meme tokens, but alas, their time has passed. It's time for KoKo!

Release Date: Presale starts in July, 2023

Category: Meme token

CONTRACT INFO

Token Name
Chicken Song

Symbol
KoKo

Contract Address
0x7d7e07fa445c70b73e8025afd15d87c4f2ea44e2

Network
Ethereum

Language
Solidity

Deployment Date
Jul 22, 2023

Verified?
Yes

Total Supply
500,000,000,000,000

Status
Not launched

TAXES

Buy Tax
1%

Sell Tax
1%

*Taxes can be changed in future

Our Contract Review Process

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

TOKEN TRANSFERS STATS

Transfer Count	1
Uniq Senders	1
Uniq Receivers	1
Total Amount	500000000000000 KoKo
Median Transfer Amount	500000000000000 KoKo
Average Transfer Amount	500000000000000 KoKo
First transfer date	2023-07-22
Last transfer date	2023-07-22
Days token transferred	1

SMART CONTRACT STATS

Calls Count	1
External calls	1
Internal calls	0
Transactions count	1
Uniq Callers	1
Days contract called	1
Last transaction time	2023-07-22 22:25:11 UTC
Created	2023-07-22 22:25:11 UTC
Create TX	0xcc53a589f58db9b9652cfa7630c74d1d7f7054a378a6058f41a7520b8704a2d4
Creator	0x70be1aea2793de4ef91b6390b878dacf0e00a5d6

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

FOUND THREATS

High Risk

Owner can set buy/sell fees up to 100%.

```
function setStructure(uint256 _percentonbuy, uint256 _percentonsell, uint256 _wallettransfer) external onlyOwner {
    sellpercent = _percentonsell;
    buypercent = _percentonbuy;
    transferpercent = _wallettransfer;
}

function setParameters(uint256 _liquidityFee, uint256 _buybackFee, uint256 _marketingFee, uint256 _devFee,
uint256 _burnFee, uint256 _feeDenominator) external onlyOwner {
    liquidityFee = _liquidityFee;
    buybackFee = _buybackFee;
    marketingFee = _marketingFee;
    devFee = _devFee;
    burnFee = _burnFee;
    totalFee = _liquidityFee.add(_buybackFee).add(_marketingFee).add(_devFee).add(_burnFee);
    feeDenominator = _feeDenominator;
    require(totalFee < feeDenominator / 2, "Fees can not be more than 50%");
    set_fees();
}

function takeFee(address sender, uint256 amount, address recipient) internal returns (uint256) {

    uint256 percent = transferpercent;
    if(recipient == pair) {
        percent = sellpercent;
    } else if(sender == pair) {
        percent = buypercent;
    }

    uint256 feeAmount = amount.mul(totalFee).mul(percent).div(feeDenominator * 100);
    uint256 burnTokens = feeAmount.mul(burnFee).div(totalFee);
    uint256 contractTokens = feeAmount.sub(burnTokens);
    _balances[address(this)] = _balances[address(this)].add(contractTokens);
    _balances[burnFeeReceiver] = _balances[burnFeeReceiver].add(burnTokens);
    emit Transfer(sender, address(this), contractTokens);


    if(burnTokens > 0){
        _totalSupply = _totalSupply.sub(burnTokens);
        emit Transfer(sender, ZERO, burnTokens);

    }

    return amount.sub(feeAmount);
}
```

- Recommendation:
  - Considered as good tax deduction practice is buy and sell fees combined not to exceed 25%.

FOUND THREATS

⚠ Medium Risk

Owner can change contract's auto swap settings.
If swapEnabled is true and swapThreshold's value is 0 and contract's token balances are 0, contract will halt on sell and selling will fail.

```
function setSwapBackSettings(bool _enabled, uint256 _amount) external onlyOwner {
    swapEnabled = _enabled;
    swapThreshold = _amount;
    emit set_SwapBack(swapThreshold, swapEnabled);
}

function shouldSwapBack() internal view returns (bool) {
    return msg.sender != pair
    && !inSwap
    && swapEnabled
    && _balances[address(this)] >= swapThreshold;
}

function _transferFrom(address sender, address recipient, uint256 amount) internal returns (bool) {
.............................
    if(shouldSwapBack()){ swapBack(); }
.............................
}

function swapBack() internal swapping {
    uint256 dynamicLiquidityFee = checkRatio(setRatio, setRatioDenominator) ? 0 : liquidityFee;
    uint256 amountToLiquify = swapThreshold.mul(dynamicLiquidityFee).div(totalFee).div(2);
    uint256 amountToSwap = swapThreshold.sub(amountToLiquify);
.........................
}
```

- Recommendation:
  - Ensure that swapThreshold's value is always above 1 token (consider decimals).

Informational

Owner can set max wallet limit but cannot lower it than 0.1% of total supply.

```
function maxWalletRule(uint256 maxWallPercent) external onlyOwner {
    require(maxWallPercent >= 1);
    _maxWalletToken = (_totalSupply * maxWallPercent ) / 1000;
    emit set_MaxWallet(_maxWalletToken);
}
```

Autoliquidity receiver (owner) will receive any tokens withdrawn from the contract. When this function is present, in cases tokens sent into the contract by mistake or purposefully, contract's owner can retrieve them.

```
function manualSend() external {
    payable(autoLiquidityReceiver).transfer(address(this).balance);

}

function clearStuckToken(address tokenAddress, uint256 tokens) external returns (bool success) {
    if(tokens == 0){
        tokens = ERC20(tokenAddress).balanceOf(address(this));
    }
    emit ClearToken(tokenAddress, tokens);
    return ERC20(tokenAddress).transfer(autoLiquidityReceiver, tokens);
}
```

RECOMMENDATIONS FOR

GOOD PRACTICES

1. Consider fundamental tradeoffs
2. Be attentive to blockchain properties
3. Ensure careful rollouts
4. Keep contracts simple
5. Stay up to date and track development

KoKo

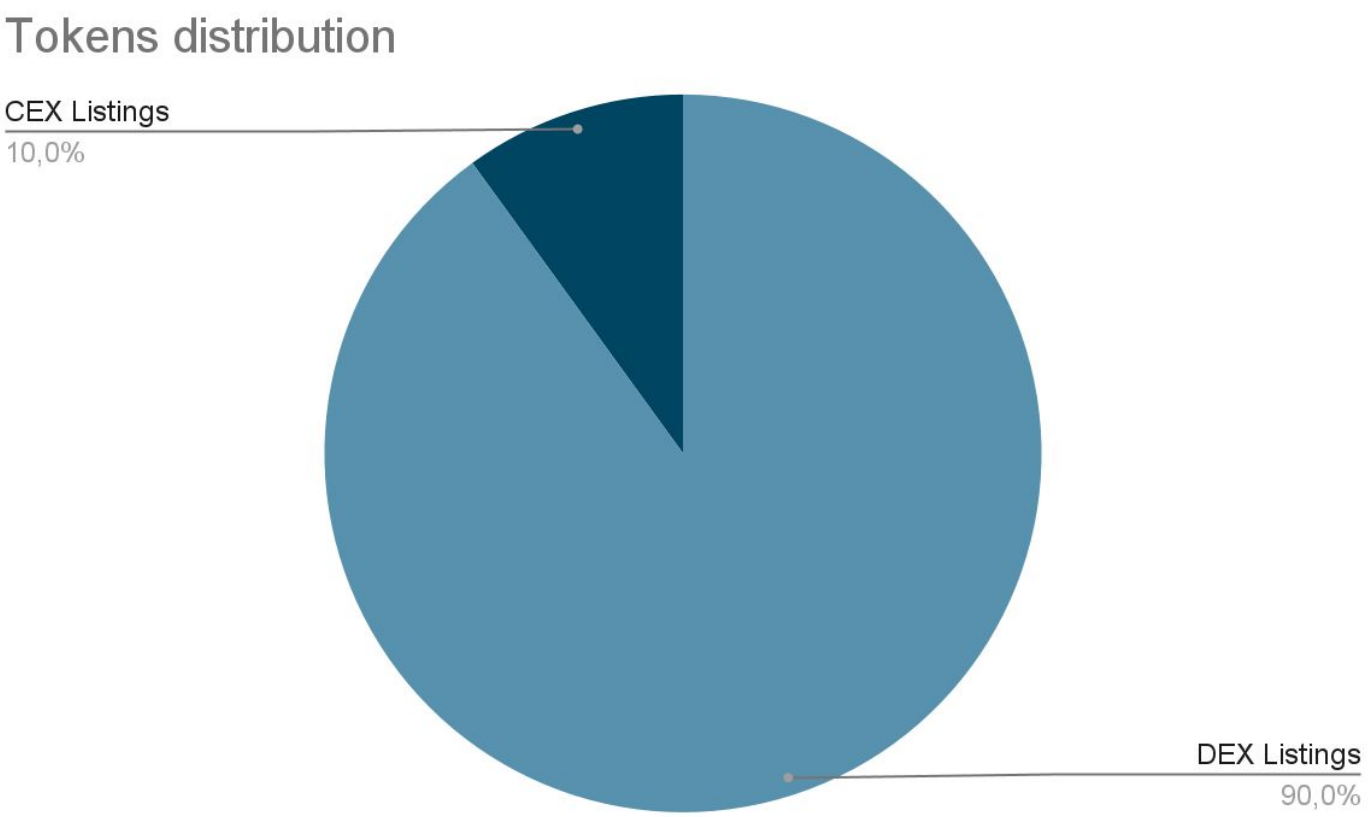
GOOD PRACTICES FOUND

- ✔ The owner cannot mint new tokens after deployment
- ✔ The owner cannot set a transaction limit but only removes it. Current max transaction limit is 1% of total supply.
- ✔ The smart contract utilizes "SafeMath" to prevent overflows

TOKENOMICS

The following tokenomics are based on the project's whitepaper and/or website:

- 90% - DEX Listings
- 10% - CEX Listings



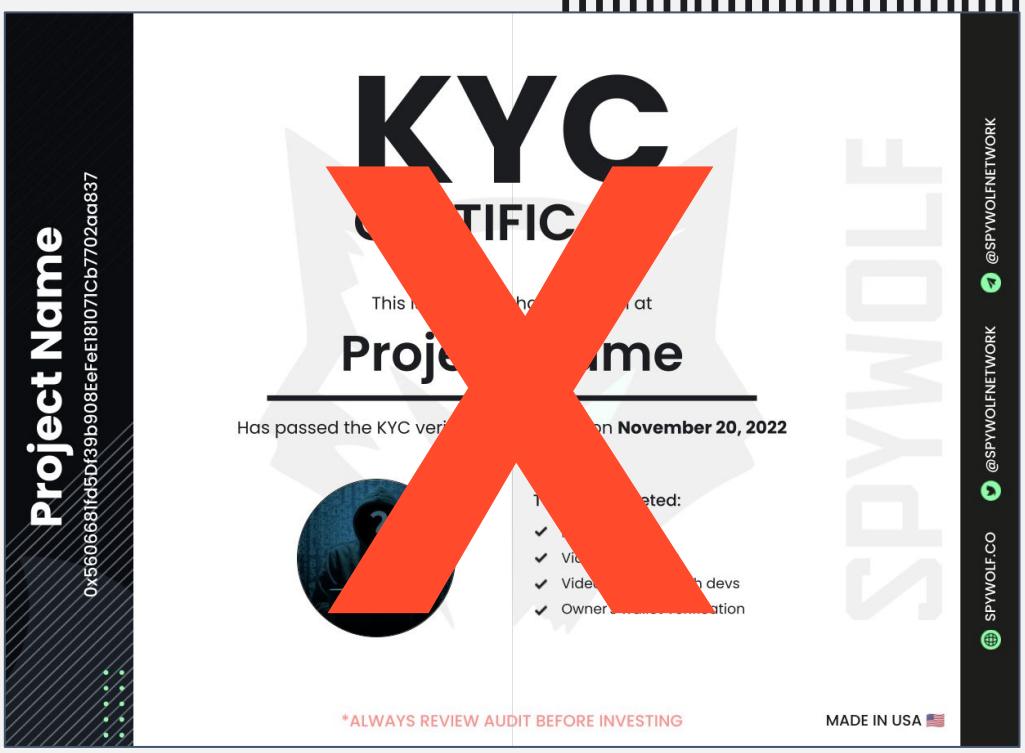
THE TEAM

⚠️ The team is annonymous

KYC INFORMATION

No KYC

We recommend the team to get a KYC in order to ensure trust and transparency within the community.



WEBSITE

Website URL
https://meme-koko.com/

Domain Registry
https://joker.com

Domain Expiration
2026-07-17

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

Design
Single page design with appropriate color scheme and graphics.

Content
The information helps new investors understand what the product does right away. No grammar mistakes found.

Whitepaper
No

Roadmap
Yes, goals set with time frames.

Mobile-friendly?
Yes

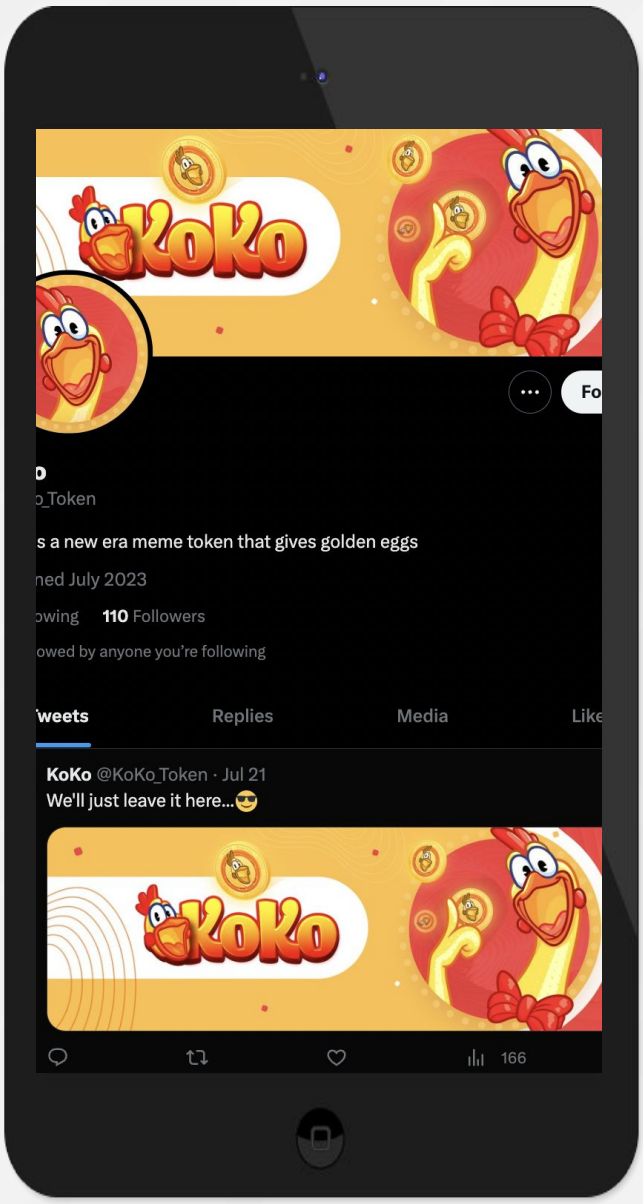
meme-koko.com

SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS

Project's social media pages are new



Twitter

@KoKo_Token

- 109 followers
- 1 Total post
- New account

Discord

- Not available

Telegram

@koko_token

- 269 members
- No posts

Medium

- Not available

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- **OVER 500 SUCCESSFUL CLIENTS**
- **MORE THAN 500 SCAMS EXPOSED**
- **MILLIONS SAVED IN POTENTIAL FRAUD**
- **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**
- **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:
By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.